AR
JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:

John G. Kennedy

Serial No. 10/092,170

Filed: March 6, 2002

For: SYSTEM AND METHOD FOR DETERMINING AVAILABILITY OF AN ARBITRARY NETWORK CONFIGURATION

§
§
§
§
§
§
§
§
§
§
§

Group Art Unit: 2145

Examiner: Hossain, Tanim M.

Atty. Dkt. No.: 5681-10100

CERTIFICATE OF MAILING
37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date indicated below:

Robert C. Kowert
Name of Registered Representative

May 24, 2006
Date

Signature

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

Further to the Notice of Appeal filed February 6, 2006 and the Notice of Panel Decision mailed April 24, 2006, Appellant presents this Appeal Brief. **This Appeal Brief is timely submitted within one month of the mailing date of the Notice of Panel Decision. Thus, no extension of time should be required.** Appellant respectfully requests that the Board of Patent Appeals and Interferences consider this appeal.

I. REAL PARTY IN INTEREST

As evidenced by the assignment recorded at Reel/Frame 012673/0369, the subject application is owned by Sun Microsystems, Inc., a corporation organized and existing under and by virtue of the laws of the State of Delaware, and now having its principal place of business at 4150 Network Circle, Santa Clara, CA 95054.

II. RELATED APPEALS AND INTERFERENCES

No other appeals, interferences or judicial proceedings are known which would be related to, directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-40 stand finally rejected. The rejection of claims 1-40 is being appealed. A copy of claims 1-40 is included in the Claims Appendix herein below.

IV. STATUS OF AMENDMENTS

No amendments to the claims have been submitted subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed toward a system comprising a network system and a plurality of network components. A host computer system is coupled to the network system and is configured to determine the availability of the network system by determining the network configuration, detecting a failure of one of its components, and determining and storing an indication of the availability of the network components. *See, e.g.,* FIG. 2, and paragraphs 0032 and 0036.

To determine the network configuration, the host computer system is configured to perform system discovery. As described in Appellant's specification, a system discovery agent executing on host 101 may be configured to perform system discovery and to provide the system discovery data to a system availability agent. In some embodiments, the system discovery agent may create a data file including the system discovery data or may provide a pointer to a data structure including the system discovery data. System discovery data may indicate a configuration of the plurality of network components and may be gathered in a variety of ways. *See, e.g.*, FIGs. 1 and 2, and paragraphs 0022-0025 and 0036. Please see the discussion of claim 7 below for a more detailed summary of the methods by which the host computer system of claim 1 may perform system discovery.

The host computer system of claim 1 is also configured to detect a failure of one of the components included in the plurality of network components. A failure detection agent, executing on host computer system 101, may be configured to detect a component failure by polling the network at regular intervals in order to detect component failures, by monitoring component performance and comparing performance to a threshold performance, or by other ways, according to various embodiments. *See, e.g.,* FIGs. 1 and 2, and paragraphs 0026 and 0036. Please see the discussion of claim 7 below for a more detailed summary of the methods by which the host computer system of claim 1 may perform detection of a component failure.

The host computer system of claim 1 is also configured to update an availability of the network system using data indicative of the configuration of the network components in response to identifying a failed component, and to store data indicative of the availability of the network system. For example, in some embodiments, a system availability agent, executing on host computer system 101, may be configured to calculate the system availability using the system discovery data, and to store an indication of the system availability. *See, e.g.,* FIGs. 1 and 2 and paragraphs 0020 and 0036. The calculation of system availability may be performed using a variety of different techniques, as described in more detail in the discussion of claim 7 below.

Independent claim 7 is directed to a computer readable medium including program instructions executable to determine availability of a network system, in a manner similar to that implemented by the host computer system of claim 1. *See, e.g.,* paragraphs 0036 and 0037. The program instructions of claim 7 are configured to implement receiving data indicating a configuration of components included in a network system. This configuration identifying data may, in some embodiments, be gathered by a system discovery agent executing on host computer system 101 or another component of the network system. This data may be used to access a lookup table or data file that indicates specifics about the physical configuration of each component, such as the number or arrangement of storage disks or the presence of spare disks in a disk array. In some embodiments, gathering the data may involve one or more components determining the makeup and configuration of a network system by examining the interconnections between components. For example, each component may have a unique ID that identifies the vendor for and/or type(s) of device(s) included in the component. The ways in which components are interconnected may also be determined through system discovery, including any fault tolerance (e.g., redundant links or redundant arrangements of components) built into the interconnect itself. In one embodiment, automated topology discovery may be performed, for example, by one component sending a Request Node Identification Data (RNID) request to each component with which it is connected. As each component responds with its unique ID, the requesting component may store the returned IDs in a link table maintained by an agent in the requesting component. Another

network component (e.g., a server) may gather identifying information from the agents in order to determine the overall topology of the system and a topology description of the network system may be written to a topology description data file or may be provided to a user graphically. See, e.g., FIG. 2 and paragraphs 0022-0025 and 0036.

The program instructions of claim 7 are also configured to implement receiving an indication of a failure of one of the components in the network system. In some embodiments, a failure detection agent executing on host computer system 101 or another component of the network system may be configured to detect a component failure and to generate the indication of the failure. This indication may be received by a system availability agent executing on host computer system 101 or another component of the network system. In one embodiment, the failure detection agent may be configured to poll the network at regular intervals or to monitor component performance and compare the performance to a threshold performance in order to determine a component failure. If a replaceable or repairable component has failed and the failed component is not currently disrupting the system (e.g., the failed component is a redundant part with at least one operable spare), the failure detection agent may be configured to notify the system availability agent of the failure. *See, e.g.,* paragraphs 0026 and 0036.

The program instructions of claim 7 are further configured to implement computing an availability of the network system from the data in response to the failure of the one of the components, and storing availability data indicative of the availability of the network system. For example, a system availability agent executing on host computer system 101 or another component may calculate system availability from the system discovery data gathered through system discovery, as described above. The availability calculation may be performed using a variety of different techniques, including using a Monte Carlo methodology, a Markov chain model, a reliability block diagram, or a fault tree. In some embodiments, the system availability agent may use the calculated system availability to calculate the risk of system disruption during one or more exposure periods, such as a period following a component failure and before the component is replaced. In some embodiments, the program instructions may be

configured to provide and/or store an indication of an unacceptably high risk of such disruption. *See, e.g.,* FIGs. 1-5, and paragraphs 0027 and 0038 – 0050.

Independent claim 23 is directed to method of operating a network system, in which network availability is determined. The method of claim 23 includes operations similar to those implemented by the program instructions of claim 7. For example, the method includes receiving data indicating a configuration of components that are included in the network system, detecting a failure of one of the components, computing an availability of the network system from the data in response to detecting the failure, and storing data indicative of the computed availability of the network system. *See, e.g.,* FIG. 2. Please see the discussion of claim 7 above for a more detailed summary of these operations of the method of claim 23.

Independent claim 34 is directed to a system including a network system that includes a plurality of components. The system includes means for determining availability of the network system in a manner similar to that of the host computing system of claim 1, the program instructions of claim 7, and the method of claim 23. For example, the system of claim 34 includes means for performing system discovery to generate data indicative of a configuration of the network system, means for detecting a failure of one of the plurality of network components, and means for calculating and storing an indication of an availability of the network system in response to detection of a component failure. *See, e.g.,* FIGs. 1 and 2. According to different embodiments, the system of claim 34 may include a host computer system 101 configured to perform these functions (as in claim 1), a computer readable medium containing program instructions configured to perform these functions (as in claim 7), or any other means to perform these functions (which correspond to the operations of the method of claim 23). Please see the discussion of claims 1 and 7 above for a more detailed summary of the functions of the system of claim 34.

Independent claim 35 is also directed to a system comprising a network system including a plurality of network components. The system of claim 35 includes a network

device coupled to the network system and configured to determine network availability. The network device of claim 35 includes a processor and a memory, such as processor 103 and memory 105 of host computer system 101. The network device of claim 35 is configured to implement determining network availability in a manner similar to that of the host computer system of claim 1. For example, the network device of claim 35 is configured to determine the availability of the network system by: determining the network configuration through system discovery, detecting a failure of one of its components, and calculating and storing an indication of the availability of the network components. The network device of claim 35 may itself be a host computer system or any other network device including a processor and memory that is so configured, according to different embodiments. For example, system availability, failure detection, and/or system discovery agents may run on other components in the system, such as on array controller 154 and/or on one or more network switches included in host/storage connection 132, instead of or in addition to running on host computer system 101, according to different embodiments. *See, e.g.,* FIG. 2 and paragraph 0036. Please see the discussion of claims 1 and 7 above for a more detailed summary of the functionality of the network device of claim 35.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-15, 22-31 and 33-36 stand finally rejected under 35 U.S.C. § 102(e) as being anticipated by Chirashnya (U.S. Publication 2002/0019870) (hereinafter "Chirashnya").

2. Claims 16-19, 32, 37 and 38 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Chirashnya.

3. Claims 20 and 21 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Chirashnya in view of Rogers (U.S. Publication 2003/0048782).

4. Claim 39 stands finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Chirashnya in view of Noy (U.S. Publication 2003/0051049).

5. Claim 40 stands finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Chirashnya in view the Examiner's "Official Notice".

VII. ARGUMENT

Claims 1, 7, 23, 34, 35 and 36:

In regard to claim 1, Chirashnya does not teach updating an availability of a network system in response to identifying a failed component, nor does Chirashnya teach using configuration data obtained via system discovery to update the availability of the network system. Claim 1 recites, in part, a host system configured to "update an availability of the network system using the data indicative of the configuration of the plurality of network components in response to identifying the failed component" and "store data indicative of the availability of the network system." In rejecting claim 1, the Examiner asserts that Chirashnya teaches these limitations, and cites paragraphs 0034, 0047, 0048, 0051 and 0059 in support of this assertion. The Examiner is incorrect in this interpretation. Chirashnya does not teach, in the cited paragraphs or anywhere else, "updating an availability of a network system in response to identifying a failed component." In fact, Chirashnya does not even teach updating the availability of a network system at all, much less updating it in response to identifying a failed component and using data indicative of the configuration of the plurality of network components, as recited in claim 1.

In response to Appellant's previous arguments regarding claim 1 (on page 9 of the Final Action), the Examiner asserts that "in receiving an alarm indicating a fault in the network system, which sets forth which component failed, for example, the user of Chirashnya's system is alerted of the network's availability, by the very fact that the user knows which component failed, which constitutes a knowledge of the network system's availability". However, a user's being "alerted" to or "knowing" "which component failed" is clearly not the same as a host system "updating an availability of the network system" using data indicative of the configuration of the plurality of network components, as recited in claim 1. Mere identification of a particular failed component of a plurality of network components does not imply that the availability of the network system is thereby somehow updated. In fact, depending on the specific configuration of

the network system, a failure of the same component may lead to completely different changes to the availability of the network system as a whole, so merely informing a user of the identity of a failed component cannot be the same as updating the availability of the network system.

In the Advisory Action mailed on February 1, 2006, the Examiner provides a somewhat different ground for rejecting claim 1, asserting that "by constructing a causal network based on the latest information gathered from any alarm (the update), probabilities of the components in the network failing are calculated, which constitutes "an availability of a network system"". The Examiner's latest interpretation of Chirashnya is also incorrect. Chirashnya's causal networks are used to update malfunction rates for individual modules, which are then compared to "expected, baseline" values for the modules (see, e.g., paragraphs 0052 and 0059). If the failure rate assessment for a given module is significantly higher than its baseline value, further action (such as module replacement or further diagnosis) is recommended. Contrary to the Examiner's suggestion, computing an updated malfunction rate for an individual module or modules does **not** constitute "updating an availability of the network system". Nowhere does Chirashnya state that an availability for the network system is updated.

The Examiner's assertion in the Advisory Action that "the collection of these parameters constitute network availability" is also incorrect. Updating malfunction rates of individual modules and/or identifying configuration changes does not mean that the availability of the network system is thereby somehow updated. Chirashnya does not teach updating or computing the availability of the network system anywhere. Nor does Chirashnya teach using configuration data obtained from a system discovery process to update the network system availability.

Further regarding claim 1, the Examiner incorrectly asserts that Chirashnya teaches "storing data indicative of the availability of the network" in paragraph 0019. However, while paragraph 0019 teaches "gathering event reports", "receiving a report of a change in configuration of the system", "constructing a causal network", "maintaining a

database in which the configuration is recorded" and "updating the database responsive to the report of the change in the configuration", it does not teach storing "data indicative of the availability of the network system". Neither recording changes to a network configuration in a database, nor constructing a "causal network", is the same as storing data indicating the availability of the network system.

Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim. M.P.E.P 2131; *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). The identical invention must be shown in as complete detail as is contained in the claims. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed above, Chirashnya clearly fails to disclose all the limitations of claim 1 and, therefore cannot be said to anticipate claim 1.

For at least these reasons, Appellant respectfully submits that claim 1 is not anticipated by Chirashnya, and is in condition for allowance. Independent claims 7, 23, 34 and 35 each also recite computing (or calculating) an availability of a network system using configuration data obtained via system discovery, and therefore the rejection of these claims is unsupported by the cited art for similar reasons as claim 1.

Claims 2, 8 and 24:

Claim 2 recites, in part, using "the updated availability to calculate a risk of the network system becoming unavailable during one or more exposure periods following the failure and prior to a repair or replacement of the failed component, and storing data indicative of the risk". The Examiner is mistaken in asserting that paragraphs 0024 and 0035 of Chirashnya teach this limitation. Neither of the cited paragraphs teaches the limitation in question. In an apparent reference to claim 2, on page 10 of the Final Action the Examiner further asserts that "the calculation of a probability of the system's failure in Chirashnya constitutes a risk of the network system becoming unavailable during the exposure period", without citing a specific portion of Chirashnya in support. Neither

paragraph 0024 nor 0035, nor any other portion of Chirashnya, however, teaches or suggests "calculation of a probability of the system's failure". Even if Chirashnya did teach such a calculation, however, the Examiner would be incorrect in the assertion that such a calculation is the same as "using the updated availability to calculate a risk of the network system becoming unavailable during one or more exposure periods following the failure and prior to a repair or replacement of the failed component", as recited in claim 2. Furthermore, Chirashnya also does not teach storing an indication of the calculated risk corresponding to the one or more exposure periods. Accordingly, claim 2 is clearly not anticipated by Chirashnya.

For at least the reasons above, the rejection of claim 2 is not supported by the cited art and removal thereof is respectfully requested. Claims 8 and 24 also recite limitations using language similar to that of claim 2, and are therefore also not anticipated by Chirashnya for similar reasons.

Claims 3, 9 and 25:

Claim 3 recites the limitation "wherein the data indicative of the risk includes data indicative of a probability of the network system becoming unavailable during each of the one or more exposure periods". The Examiner incorrectly asserts that Chirashnya teaches this limitation in paragraph 0010. There is no teaching or suggestion in paragraph 0010 or anywhere else in Chirashnya of using an updated availability of a network system to calculate and store probabilities of the network system becoming unavailable during one or more exposure periods between the failure and a repair/replacement. Accordingly, claim 3 is also not anticipated by Chirashnya.

For at least these reasons, the rejection of claim 3 is not supported by the cited art and removal thereof is respectfully requested. Claims 9 and 25 are also not anticipated by Chirashnya for similar reasons.

Claims 4, 10 and 26:

Claim 4 recites "wherein the data indicative of the risk includes data indicative of an expected number of system failures per a given population for each of the one or more exposure periods". In rejecting claim 4, the Examiner cites paragraph 0026 of Chirashnya as teaching this limitation. The Examiner is mistaken. While paragraph 0026 teaches "failure rate distributions", these failure rate distributions are for "malfunctions" of individual modules (see, e.g., paragraph 0023s, 0054), not "system failures" as recited in claim 4. Furthermore, paragraph 0026 does not teach failure rate distributions associated with each of one or more respective "exposure periods". In addition, Chirashnya teaches (e.g., in paragraph 0054) that "failure rates" are expressed as "mean time between failures (MTBF)", which is different from the "number of failures per a given population" for a given exposure period.

For at least these reasons, claim 4 is not anticipated by Chirashnya, and removal of the rejection thereof is respectfully requested. Claims 10 and 26 are also not anticipated by Chirashnya for similar reasons.

Claim 5:

Claim 5 recites a host computer system configured, in part, to "determine an acceptable exposure period, wherein the risk of the network system becoming unavailable during the acceptable exposure period is lower than the threshold value, and provide an indication of the acceptable exposure period". The Examiner is incorrect in asserting that paragraphs 0020, 0022, 0027, 0054 and 0063 of Chirashnya teach the combination of limitations of claim 5. None of the cited portions, or any other portion of Chirashnya, teach determining an acceptable exposure period with a lower risk of the network system becoming unavailable than a threshold risk value, and providing an indication of the acceptable exposure periods. The "updated probabilities" of paragraph 0027 refer to probabilities of malfunctions of individual components, not "risks of the network system becoming unavailable" during specific "exposure periods". Furthermore, "providing an

explanation of the diagnosis" as taught in paragraph 0027 is different from "providing an indication of an acceptable exposure period". Paragraph 0063 teaches "Preferably, the user defines two threshold levels that are applied to each module: a lower threshold, at which a module is flagged as 'fault-suspect,' and a higher threshold, at which a suspect module is reclassified as non-suspect. The thresholds relate to the difference between the assessed malfunction rate of each module and its expected failure rate based on system specifications." These "two threshold levels" of paragraph 0063 clearly have nothing to do with determining an acceptable exposure period or providing an indication of such an acceptable exposure period, as recited in claim 5. Claim 5 is therefore clearly not anticipated by Chirashnya and removal of the rejection thereof is respectfully requested.

Claim 6:

Claim 6 recites "wherein the host computer system is configured to update the availability of the network system by calculating the instantaneous availability of the plurality of network components". The Examiner suggests that Chirashnya teaches this limitation in paragraphs 0011 and 0048. The Examiner is incorrect in this interpretation as well. Chirashnya does not teach a host updating the availability of the network system anywhere, and so cannot teach that the network system availability is updated by calculating the instantaneous availability of the plurality of network components, as recited in claim 6. Claim 6 is therefore clearly not anticipated by Chirashnya and removal of the rejection thereof is respectfully requested.

Claims 11 and 31:

With respect to claim 11, the Examiner is mistaken in asserting that paragraph 0054 of Chirashnya teaches the limitation of "wherein a first exposure period of the one or more exposure periods is an estimated time to replace the one of the components that failed". Chirashnya does not mention "estimated times" to replace any components anywhere, much less setting an exposure period in a table to the estimated time to replace a failed component. Accordingly, claim 11 is clearly not anticipated by Chirashnya and

removal of the rejection thereof is respectfully requested. Claim 31 is also not anticipated by Chirashnya for similar reasons.

Claims 12 and 27:

Regarding claim 12, contrary to the Examiner's assertion, Chirashnya clearly fails to disclose the limitation "the program instructions are computer executable to evaluate the risk of the network system being disrupted by comparing the risk of the network system being disrupted for at least one of the one or more exposure periods to a threshold risk" in paragraphs 0047 and 0063. Paragraph 0047 does describe setting error thresholds used in deciding when to generate an alarm in response to a suspected error in an individual component. Paragraph 0063 describes both a lower threshold (indicating a "fault suspect") and an upper threshold (indicating that a suspect module should be reclassified as non-suspect). However, these thresholds relate to mean time between failure (MTBF) rates, not risk levels. Neither of these citations discloses evaluating a risk of the network being disrupted, comparing this risk to a threshold risk, or the network system being disrupted during at least one of one or more "exposure periods" as recited in claim 12. Therefore Chirashnya cannot be said to anticipate claim 12.

For at least the reasons above, the rejection of claim 12 is not supported by the cited art and removal thereof is respectfully requested. Claim 27 is also not anticipated by Chirashnya for similar reasons.

Claims 13 and 28:

Regarding claim 13, contrary to the Examiner's assertion, Chirashnya clearly fails to disclose the limitation "the program instructions are computer executable to store an indication of an unacceptably high risk in response to the risk of the network system being disrupted for at least one of the one or more time periods being greater than the threshold risk" in paragraph 0048. This paragraph describes event collectors, which gather system events on various nodes and send them to a primary event collector for

processing. Thus, this passage describes actions taken after occurrence of an actual system event. This clearly has nothing to do with a risk of a network system disruption, or with storing an indication of an unacceptably high risk, much less with storing such an indication in response to the risk of the network system being disrupted being greater than a threshold risk, as recited in claim 13. Therefore, Chirashnya clearly does not anticipate claim 13.

For at least the reasons above, the rejection of claim 13 is not supported by the cited art and removal thereof is respectfully requested. Claim 28 is also not anticipated by Chirashnya for similar reasons.

Claims 14 and 29:

Regarding claim 14, contrary to the Examiner's assertion, Chirashnya clearly fails to disclose the limitation "the indication of the unacceptably high risk includes an indication of an acceptable exposure period" in paragraph 0054. This passage describes a fault model that includes all types of possible malfunctions (where "malfunctions" refers to the root cause of some fault in a module) and their expected failure rates, such as the mean time between failures these root causes. It does not describe an indication of an unacceptably high risk (of the network system being disrupted) at all, much less one including an indication of an "acceptable exposure period", as recited in claim 14. Therefore, claim 14 is clearly not anticipated by Chirashnya.

For at least the reasons above, the rejection of claim 14 is not supported by the cited art and removal thereof is respectfully requested. Claim 29 is also not anticipated by Chirashnya for similar reasons.

Claims 15 and 30:

Regarding claim 15 and contrary to the Examiner's assertion, Chirashnya clearly fails to disclose the limitation "the program instructions are computer executable to

provide the acceptable exposure period to a monitoring service" in paragraph 0059. This passage describes "a recommendation and explanation generator" receiving malfunctions assessments for the modules in the network and comparing them against expected failure rates to determine a recommended action, such as running additional diagnostics or replacing the module. This has nothing to do with providing an acceptable exposure period (included in an indication of an unacceptably high risk) to a monitoring service, as recited in claim 15. Therefore, Chirashnya cannot be said to anticipate claim 15.

For at least the reasons above, the rejection of claim 15 is not supported by the cited art and removal thereof is respectfully requested. Claim 30 is also not anticipated by Chirashnya for similar reasons.

Claims 16-19, 32, 37 and 38:

With respect to claims 16-19, 32, 37 and 38, the Examiner asserts that the features of claims 16-19 and 32 "constitute a design choice rather than a patentable distinction." The Examiner has repeatedly failed to state proper grounds for rejection. All inventions constitute design choices made by the inventors. The statute clearly places a burden of proof on the Patent Office that requires the Examiner to produce a factual basis for his rejection of an application under sections 102 and 103. *In re Warner*, 154 USPQ 173, 177 (C.C.P.A. 1967), *cert. denied*, 389 U.S. 1057 (1968). The Examiner's statement that these claim features are a matter of design choice is a conclusory statement with no factual basis. **The Examiner has not provided any evidence of record establishing the obviousness of the recited claim limitations in combination with the other limitations of Appellant's claimed invention.** The Examiner has merely stated his own opinion, which by definition does not provide a factual basis for the rejection. As the Court of Appeals for the Federal Circuit recently explained in *In re Sang Su Lee*, Docket No. 00-1158 (Fed. Cir. January 18, 2002), "conclusory statements such as those provided by the Examiner that a claim limitation is only a design choice do not fulfill the Examiner's obligation." "Deficiencies of the cited references cannot be remedied by the [Examiner's] general conclusions about what is 'basic knowledge' or 'common sense.'"

In re Zurko, 59 USPQ2d 1693, 1697 (Fed. Cir. 2001). "Common knowledge and common sense ... do not substitute for authority." *In re San Su Lee*. Common knowledge "does not in and of itself make it so" absent evidence of such knowledge. *Smiths Industries Medical Systems, Inc. v. Vital Signs, Inc.*, 51 USPQ2d 1415, 1421 (Fed. Cir. 1999). The Examiner's rejection of claims 37 and 38 is also completely lacking any evidentiary support. Thus, the Examiner has failed to state a *prima facie* rejection of claims 16-19, 32, 37 and 38, and removal of the rejection thereof is respectfully requested.

Claims 20 and 21:

With respect to claims 20 and 21, in response to the Office Action dated May 18, 2005, Appellant had indicated **two** requirements that had to be met for Rogers' teachings to qualify as prior art. These two requirements were: first, that the Examiner must show that the subject matter on which the Examiner is relying on to reject Appellant's claims is also present in Rogers' provisional application or Rogers' parent utility application, and second, that at least one claim of Rogers' published application is supported (under 35 U.S.C. § 112) in a respective one of the priority applications that also includes the subject matter relied upon for the rejection. In the Final Action and again in the Advisory Action, the Examiner addresses the first requirement, stating "that the provisional application contains the exact same teachings as the published Rogers application used to reject claims 20 and 21", **but does not address the second requirement.** In regard to the first requirement, Appellant notes that, contrary to the Examiner's statement, the text of the provisional application does not appear to be identical to the text of the published application. **In regard to the second requirement, the Examiner has not even attempted to show that at least one claim of Rogers' published application is supported (under 35 U.S.C. § 112) in a respective one of the priority applications that also includes the subject matter relied upon for the rejection. Thus, the Examiner has not met the burden required to qualify the use of Rogers as prior art, and the rejection of claims 20 and 21 remains improper.** For each and every limitation of at least one claim of Roger's published application, the Examiner must

specifically identify in the priority document complete § 112 support. Otherwise, Rogers cannot be asserted as prior art. For at least these reasons, removal of the rejection of claims 20 and 21 is respectfully requested.

Claims 22 and 33:

Regarding claim 22 and contrary to the Examiner's assertion, Chirashnya fails to disclose the limitation "the program instructions are computer executable to compute the availability of the network system by computing the instantaneous availability of the network system" in paragraph 0010. This passage describes estimated malfunction rates of a given module exceeding a threshold, resulting in the system declaring the module to be fault-suspect. It does not describe that such a declaration has anything to do with the availability of the network system, nor that such availability is computed instantaneously or otherwise. Thus, Chirashnya clearly does not anticipate claim 22.

For at least the reasons above, the rejection of claim 22 is not supported by the cited art and removal thereof is respectfully requested. Claim 33 is also not anticipated by Chirashnya for similar reasons.

Claim 39:

The Examiner rejected claim 39 under 35 U.S.C. § 103(a) as being unpatentable over Chirashnya in view of Noy (U.S. Publication 2003/0051049). Appellant traverses this rejection for several reasons. First, the Examiner has not shown Noy to be a prior art reference. More specifically, Noy is a published U.S. patent application that was filed on Aug. 13, 2002, after Appellant's filing date of Mar. 6, 2002. Noy does claim the benefit of a provisional application filed Aug. 15, 2001. However, the filing date of the provisional application can only be used as Noy's prior art date for the subject matter that is common to both the published application and the provisional application. Since it is common practice for a later filed utility application to include more or different subject matter than its earlier provisional application, it is unclear whether the material in Noy

relied upon by the Examiner was actually present in Noy's provisional application. In fact, a quick review of Noy's provisional application shows that it varies greatly from Noy's published application. Therefore, Appellant asserts that the Examiner must show that the subject matter on which the Examiner is relying on to reject Appellant's claims is also present in Noy's provisional application. Because the Examiner has failed to make this showing, the rejection is clearly improper. *See, In re Wertheim*, 209 USPQ 554 (CCPA 1981).

Moreover, Noy's published application is not entitled to the filing date of the provisional application unless at least one claim of Noy's published application is supported (under 35 U.S.C. § 112) in the provisional application. Under 35 U.S.C. 119(e)(1) and/or 120, a published utility application is not entitled to its priority application's filing date as a prior art date unless at least one claim of the published utility application is supported (per 35 U.S.C. § 112) in the priority application. The rejection is improper unless the Examiner can show that Noy's published application has the necessary claim support in the provisional application. *See also* M.P.E.P. § 2136.03(IV).

The Examiner has the burden of proof to produce the factual basis for the rejection. *In re Warner*, 154 USPQ 173, 177 (C.C.P.A. 1967), *cert. denied*, 389 U.S. 1057 (1968). **Since the Examiner has not proven that both of the above requirements have been met for Noy's teachings to qualify as prior art, the Examiner has not met this burden of proof and the rejection is improper.**

Further regarding claim 39, the Examiner asserts, while Chirashnya "does not specifically teach that system discovery entails sending a request for identification of the network component, and returning an identifier in response", Noy teaches "the unique identification of a network component by request (0008)". The Examiner is mistaken in this interpretation. Claim 39 recites "wherein said performing system discovery comprises sending a request for identification data to a particular network component of the plurality of network components; and the particular network component returning a unique identifier in response to the request for identification". Noy teaches "sending

from a device component **within a model** of a computer network to each of its neighboring device components via outgoing links a path discovery request" (paragraph 0008), but this is very different from a host sending a request for identification data to a network component. Each "device component" of Noy **models** "one or more physical and/or logical aspects of a network element" (see, e.g., paragraph 0005) included within a "software and/or hardware agent" defined for the network element (paragraph 0005), and is **not** "a network component of a plurality of network components" forming a network system whose availability is updated using the configuration data obtained via system discovery, as recited in claim 39.

Still further, the Examiner's suggested motivation for combining the teachings of Noy with those of Chirashnya is clearly insufficient. The Examiner suggests that the motivation lies "in the fact that identification of the components would enable more efficient monitoring of the components, which would facilitate response in case of a failure". However, the Examiner presents no evidence of a link between "identification" and alleged increased "efficiency of monitoring" of components. Appellant respectfully submits that "monitoring" a component without "identifying" the component does not make sense (exactly what would be monitored?), and that identification of components therefore cannot enable "more efficient monitoring" as suggested by the Examiner, and that the Examiner's suggested reasoning for combining the teachings of Noy and Chirashnya is therefore flawed.

For at least the reasons cited above, the rejection of claim 39 is clearly unsupported by the art cited by the Examiner even if Noy were properly qualified as prior art.

Claim 40:

With respect to claim 40, the Examiner cites paragraph 0009 of Chirashnya as teaching "wherein said detecting the failure comprises monitoring performance of one of the components", and takes Official Notice that "inclusion of a threshold value to

determine component failure is well known in the art, wherever network performance is being monitored". Pursuant to M.P.E.P. § 2144.03, Appellant have traversed the Examiner's taking of Official Notice. Appellant asserts that "determining that the one of the network components has failed if the performance falls below a threshold" as recited in claim 40 is not "well known in the art". **The Examiner has failed to provide documentary evidence for the Official Notice taken in the rejection of this claim.** Therefore, pursuant to M.P.E.P. § 2144.03, the rejection of claim 40 must be withdrawn.

In addition, while paragraph 0009 of Chirashnya teaches that "standard reliability theory techniques are based on sampling device performance under known conditions", this is not the same as the detection of a failure of a component comprising "monitoring performance of the component", as recited in claim 40. For at least these reasons, the rejection of claim 40 is clearly unsupported by the art cited by the Examiner and removal thereof is respectfully requested.

VIII. CONCLUSION

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1-40 was erroneous, and reversal of his decision is respectfully requested.

The Commissioner is authorized to charge the appeal brief fee of $500.00 and any other fees that may be due to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5681-96802/RCK. This Appeal Brief is submitted with a return receipt postcard.

Respectfully submitted,

Robert C. Kowert
Reg. No. 39,255
Attorney for Appellant

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
(512) 853-8850

Date: May 24, 2006

IX. CLAIMS APPENDIX

The claims on appeal are as follows.

1. A system, comprising:

a network system comprising a plurality of network components;

a host computer system coupled to the network system, wherein the host computer system is configured to:

perform system discovery to generate data indicative of a configuration of the plurality of network components;

detect a failure of one of the components included in the plurality of network components;

in response to identifying the failed component, update an availability of the network system using the data indicative of the configuration of the plurality of network components; and

store data indicative of the availability of the network system.

2. The system of claim 1, wherein the host computer system is configured to use the updated availability to calculate a risk of the network system becoming unavailable during one or more exposure periods following the failure and prior to a repair or replacement of the failed component, and store data indicative of the risk.

3. The system of claim 2, wherein the data indicative of the risk includes data indicative of a probability of the network system becoming unavailable during each of the one or more exposure periods.

4. The system of claim 2, wherein the data indicative of the risk includes data indicative of an expected number of system failures per a given population for each of the one or more exposure periods.

5. The system of claim 2, wherein the host computer system is configured to:

compare the risk of the network system becoming unavailable for a first exposure period of the one or more exposure periods to a threshold value; and

if the risk is higher than the threshold value, determine an acceptable exposure period, wherein the risk of the network system becoming unavailable during the acceptable exposure period is lower than the threshold value, and provide an indication of the acceptable exposure period.

6. The system of claim 1, wherein the host computer system is configured to update the availability of the network system by calculating the instantaneous availability of the plurality of network components.

7. A computer readable medium, comprising program instructions computer executable to:

receive data indicating a configuration of components included in a network system;

receive an indication of a failure of one of the components in the network system;

compute an availability of the network system from the data in response to the failure of the one of the components, and

store availability data comprising data indicative of the availability of the network system.

8. The computer readable medium of claim 7, wherein the availability data comprises a table comprising one or more entries, wherein each entry in the table indicates a risk of the network system being disrupted during a respective exposure period following the failure and prior to a repair or replacement of the failed component, wherein the risk depends on the availability of the network system.

9. The computer readable medium of claim 8, wherein each entry in the table indicates a probability of the network system being disrupted during the respective exposure period.

10. The computer readable medium of claim 8, wherein each entry in the table indicates an expected number of system failures per a given population for the respective exposure period.

11. The computer readable medium of claim 8, wherein a first exposure period of the one or more exposure periods is an estimated time to replace the one of the components that failed.

12. The computer readable medium of claim 7, wherein the program instructions are computer executable to evaluate the risk of the network system being disrupted by comparing the risk of the network system being disrupted for at least one of the one or more exposure periods to a threshold risk.

13. The computer readable medium of claim 12, wherein the program instructions are computer executable to store an indication of an unacceptably high risk in response to the risk of the network system being disrupted for at least one of the one or more time periods being greater than the threshold risk.

14. The computer readable medium of claim 13, wherein the indication of the unacceptably high risk includes an indication of an acceptable exposure period.

15. The computer readable medium of claim 14, wherein the program instructions are computer executable to provide the acceptable exposure period to a monitoring service.

16. The computer readable medium of claim 7, wherein the program instructions are computer executable to calculate the availability using reliability block diagram analysis.

17. The computer readable medium of claim 7, wherein the program instructions are computer executable to calculate the availability using fault tree analysis.

18. The computer readable medium of claim 7, wherein the program instructions are computer executable to calculate the availability using Monte Carlo analysis.

19. The computer readable medium of claim 7, wherein the program instructions are computer executable to calculate the availability using Markov chain analysis.

20. The computer readable medium of claim 7, wherein the program instructions are computer executable to calculate the availability of a group of non-redundant components by multiplying individual availabilities of each non-redundant component in the group.

21. The computer readable medium of claim 20, wherein at least one of the non-redundant components includes a plurality of redundant components.

22. The computer readable medium of claim 7, wherein the program instructions are computer executable to compute the availability of the network system by computing the instantaneous availability of the network system.

23. A method of operating a network system, the method comprising:

receiving data indicating a configuration of components that are included in the network system;

detecting a failure of one of the components;

computing an availability of the network system from the data in response to said detecting; and

storing data indicative of the availability of the network system generated by said computing.

24. The method of claim 23, further comprising storing data indicative of a risk of the network system being disrupted during one or more exposure periods following the failure and prior to a repair or replacement of the failed component, wherein the risk depends on the availability of the network system.

25. The method of claim 24, wherein the data indicative of the risk includes data indicative of a probability of the network system being disrupted during each of the one or more exposure periods.

26. The method of claim 24, wherein the data indicative of the risk includes data indicative of an expected number of system failures per a given population for each of the one or more exposure periods.

27. The method of claim 24, further comprising comparing the risk of the network system being disrupted for at least one of the one or more exposure periods to a threshold risk.

28. The method of claim 27, further comprising storing an indication of an unacceptably high risk in response to the risk of the network system being disrupted for at least one of the one or more exposure periods being greater than the threshold risk.

29. The method of claim 28, wherein the indication comprises an indication of an acceptable exposure period.

30. The method of claim 29, further comprising providing the indication of the acceptable exposure period to a monitoring service.

31. The method of claim 24, wherein a first exposure period of the one or more exposure periods is an estimated time to replace the one of the components that failed.

32. The method of claim 23, wherein said computing comprises calculating the availability using reliability block diagram analysis.

33. The method of claim 23, wherein said computing comprises calculating the instantaneous availability of the network system.

34. A system comprising:

a network system comprising a plurality of components;

means for performing system discovery for the network system, wherein the means for performing system discovery generate data indicative of a configuration of the network system;

means for detecting a failure of one of the plurality of network components; and

means for calculating an availability of the network system from the data generated by the means for performing system discovery, wherein the

means for calculating an availability calculate the availability in response to the means for detecting a failure detecting that a first one of the plurality of network components has failed, wherein the means for calculating the availability store data indicative of the availability of the network system.

35. A system, comprising:

a network system comprising a plurality of network components;

a first network device coupled to the network system, wherein the first network device includes a processor and a memory, wherein the first network device is configured to:

perform system discovery to generate data indicative of a configuration of the plurality of network components;

detect a failure of one of the components included in the plurality of network components;

in response to detecting the failure, calculate an availability of the network system using the data indicative of the configuration of the plurality of network components; and

store data indicative of the availability of the network system.

36. The system of claim 35, wherein the first network device is a host computer system.

37. The system of claim 35, wherein the first network device is an array controller.

38. The system of claim 35, wherein the first network device is a network switch.

39. The system of claim 1, wherein said performing system discovery comprises:

sending a request for identification data to a particular network component of the plurality of network components; and

the particular network component returning a unique identifier in response to the request for identification.

40. The system of claim 1, wherein said detecting the failure comprises:

monitoring performance of the one of the components; and

determining that the one of the components has failed if the performance falls below a threshold.

X. EVIDENCE APPENDIX

No evidence submitted under 37 CFR §§ 1.130, 1.131 or 1.132 or otherwise entered by the Examiner is relied upon in this appeal.

XI. RELATED PROCEEDINGS APPENDIX

There are no related proceedings.